

# 攻防世界 flag\_in\_your\_hand

原创

仲璧 于 2022-03-11 16:59:15 发布 1295 收藏 1

分类专栏: [CTF](#) 文章标签: [javascript](#) [safari](#) [webview](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/m0\\_49025459/article/details/123424876](https://blog.csdn.net/m0_49025459/article/details/123424876)

版权



[CTF 专栏收录该内容](#)

50 篇文章 1 订阅

订阅专栏

## flag\_in\_your\_hand

最佳Writeup由 [清流](#) · [ArmeY](#) 提供

难度系数: ☆☆2.0

题目来源: [CISCN-2018-Quals](#)

题目描述: 暂无

题目场景: 暂无

题目附件: [附件1](#)

CSDN @壬二舟

下载附件打开文件中的html文件

## Flag in your Hand

Type in some token to get the flag.

Tips: Flag is in your hand.

Token:

CSDN @壬二舟

无论输入什么都是错误

# Flag in your Hand

Type in some token to get the flag.

Tips: Flag is in your hand.

Token:

Get flag!

Wrong!

xMpCOKKC5I4INzFCab3WEmw  
CSDN @壬二舟

我们打开网页源代码看看

```
<html>
<head>
<title>Flag in your Hand</title>
<style type="text/css">
  body {
    padding-left: 30%;
  }

  #flag {
    font-family: Garamond, serif;
    font-size: 36px;
  }

  #flagtitle {
    font-family: Garamond, serif;
    font-size: 24px;
  }

  .rightflag {
    color: green;
  }

  .wrongflag {
    color: red;
  }
</style>
<script src="script-min.js"></script>
<script type="text/javascript">
  var ic = false;
  var fg = "";

  function getFlag() {
    var token = document.getElementById("secToken").value;
    ic = checkToken(token);
    fg = bm(token);
    showFlag()
  }
</script>
</html>
```

```

}

function showFlag() {
  var t = document.getElementById("flagTitle");
  var f = document.getElementById("flag");
  t.innerText = !!ic ? "You got the flag below!!" : "Wrong!";
  t.className = !!ic ? "rightflag" : "wrongflag";
  f.innerText = fg;
}
</script>
</head>
<body>
<h1>Flag in your Hand</h1>
<p>Type in some token to get the flag.</p>
<p>Tips: Flag is in your hand.</p>
<div>
  <p>
    <span>Token:</span>
    <span><input type="text" id="secToken"/></span>
  </p>
  <p>
    <input type="button" value="Get flag!" onclick="getFlag()" />
  </p>
</div>
<div>
  <p id="flagTitle"></p>
  <p id="flag"></p>
</div>
</body>
</html>

```

## 获得flag

```

function getFlag() {
  var token = document.getElementById("secToken").value;
  ic = checkToken(token);
  fg = bm(token);
  showFlag()
}

```

## 输出flag

```

function showFlag() {
  var t = document.getElementById("flagTitle");
  var f = document.getElementById("flag");
  t.innerText = !!ic ? "You got the flag below!!" : "Wrong!"; //判断ic是true还是false
  t.className = !!ic ? "rightflag" : "wrongflag";
  f.innerText = fg;
}

```

然后我们查看[script-min.js](#)其中改变ic的值的

```

function ck(s) {
  try {
    ic
  } catch (e) {
    return;
  }
  var a = [118, 104, 102, 120, 117, 108, 119, 124, 48,123,101,120];
  if (s.length == a.length) {
    for (i = 0; i < s.length; i++) {
      if (a[i] - s.charCodeAt(i) != 3)
        return ic = false;
    }
    return ic = true;
  }
  return ic = false;
}

```

我们读代码发现当a-我们输入的字符串等于3的时候ic就是true所以我们把它翻过来我这里用python写的

```

a=[118, 104, 102, 120, 117, 108, 119, 124, 48, 123, 101, 120]
b=''
for i in a:
  b+=chr(i-3)
print(b)

```

运行一下

The screenshot shows an online Python3 IDE interface. At the top, there are buttons for '点击运行' (Click to Run), '标准输入(stdin)' (Standard Input), '多个输入值?' (Multiple Input Values?), 'Python3 在线工具' (Python3 Online Tools), '复制' (Copy), and '清空' (Clear). On the right, there is a '邮件反馈' (Email Feedback) button. The main area is split into two panes: the left pane contains the Python code, and the right pane shows the output 'security-xbu'. At the bottom right of the IDE, there is a watermark 'CSDN @千二舟'.

得出结果

```
security-xbu
```

我们返回html输入这个值

# Flag in your Hand

Type in some token to get the flag.

Tips: Flag is in your hand.

Token:

You got the flag below!!

RenIbyd8Fgg5hawvQm7TDQ

CSDN @壬二舟

就得出了，flag

RenIbyd8Fgg5hawvQm7TDQ



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)